TOP SECRET

TICOM/I-197

FURTHER INTERROGATION OF AMTSRAT SHULZE OF OKM/4 SKL III

Attached is a report on a further interrogation of Amtsrat SCHULZE carried out at HAMBURG on 28/29 May, 1946, by Major G.K. BROWN, I.C., to obtain replies to questions set by OP-20-G and L.S.I.C. mainly on American and British Naval Machine Traffic.

2. Questions on certain points in connection with British Machine Cyphers necessitated further interrogation of Oberreg: TRANOW whose replies have been incorporated in this report.

3. Previous reports on the interrogation of SCHULZE were issued as Ticom/I-141 and Ticom/I-147.

4. The remarks in para 2 regarding "TBC" result from a corruption of the original request, which was for "ABC" (E.C.M.). "Verfahren ULM" is the C.C.M. and "DUPYH" a U.S. Naval Strip System.

Ticom
2nd July, 1946.

No. of Pages: 8

Distribution:

L.S.I.C.

T
S
H
M
L
Z
71
63 for Dr. C.W. Morgan
86
91
Ticom Files (4 copies)

U.S.

U.S.L.O.
OP-20-G (4 copies) } via
A.S.A. (4 copies) } U.S.L.O.
Director, A.S.A, Europe)

Additional

91 for D.S.D.10, Admiralty.

TICOM/I-197

TOP SECRET

INTERROGATION REPORT ON AMTSRAT SCHULZE.

DATE OF INTERROGATION: 28/29 May, 1946.

PLACE OF INTERROGATION: HAMBURG.

OFFICER CARRYING OUT INTERROGATION: MAJOR G.K. BROWN, INT. CORPS.

I. General

SCHULZE now works with No. 10 GERMAN NEWS SERVICE at ROTHENBAUM STR. 169, HAMBURG, which is run by a BRITISH official, Mr. MORGAN (Telephone No. 555846, Extension 35). In carrying out the investigation it was also found necessary to interrogate OBERREGIERUNGSRAT TRANOW on various points regarding BRITISH ciphers.

II. Detailed Interrogation

1. Organisation of Abteilung 4 SKL III

(i) Numbers of personnel. In the whole of 4 SKL III there were in the middle of 1942 as many as 1100 people engaged. The English ciphers section under ORR TRANOW at this time numbered 730. SCHULZE's American section numbered 52 but was later reduced to about 20. General reductions of personnel were becoming progressively larger in 1944 and 1945, as more and more of the personnel were sent to the front. SCHULZE also lost personnel to KORVETTENKAPITAEN SINGER, of whom more later.

(ii) Departments. Head of III was KAPITAEN ZUR SEE KUPFER. IIIa, b, i and k were concerned with co-ordinating the results of cipher breaks, etc. The heads of these sections were respectively FREGATTEN KAPITAEN VON VOIGT, KORVETTEN KAPITAEN HERMANN, KORVETTEN KAPITAEN BERINGUIER and AMTSRAT BUCHHOLZ.

(iii) Section IIIF. This was controlled by ORR TRANOW who was concerned with all research on ENGLISH NAVAL Codes and Ciphers. The section was sub-divided into IIIFn, under RR Dr. THOMA (who was responsible for FLEET Code, NAVAL Code- Subtractor Code, MERCHANT NAVY Code, etc). IIIFm (RR Dr. SCHEURLE - Verfahren STETTIN and ULM,) IIIFq (OBLTN. KOLLWITZ - LOXO, COFOX, MEDOX, etc).

Section IIIr controlled by KPT LTN. HARMANN, dealt entirely with RUSSIA. HARMANN was a German Russian and SCHULZE last saw him in the EBERSWALDE area.

Section IIIu controlled by SCHULZE, dealt with research on USA NAVAL traffic, particularly on the HAGELIN machine, and on FRENCH and SWEDISH traffic.

Section IIIv controlled by ORR FRANKE. FRANKE was SCHULZE's predecessor as head of IIIu, but was apparently replaced by SCHULZE owing to his increasing lack of success and new ideas. Section IIIv merely assisted IIIu and FRANKE was eventually in December 1944 posted to OKH. SCHULZE last saw him in January 1945 at EBERSWALDE and thinks he stayed in BERLIN after the collapse.

Please turn over

TOP SECRET

2. Verfahren ULM, TBC and TYPEX.

Work on these systems was carried out under the direction of TRANOW, although SCHULZE from time to time undoubtedly gave some assistance.

(i) Verfahren ULM. A new machine cipher began to be intercepted in April 1944. Traffic came from the south and south-east coastal areas and was assumed to be convoy traffic. It was regarded as one more pointer to the imminent invasion.

Deviation Percentage and Z-Strip investigations established that the machine was neither TYPEX or HAGELIN. 20 men plus a HOLLERITH component worked on the new cipher for six weeks, and then gave it up. Other matters at this time were more pressing and personnel was too short.

(ii) Verfahren TBC. Neither SCHULZE nor TRANOW was too clear as to what was meant by TBC, but guessed, reasonably enough, that the Tactical Bomber Code was referred to. This code was extremely simple, and was read currently. It was eventually handed over to the LUFTWAFFE. No HOLLERITH component, of course, was used in breaking.

(iii) TYPEX. Quite obviously, the main effort on TYPEX was made elsewhere, probablyat OKW/Chi. Nevertheless, TRANOW and SCHULZE both from time to time investigated its characteristics, mainly because TYPEX traffic increasingly appeared on NAVAL links. The eventual conclusion of 4 SKL III (and according to TRANOW, of OKH and OKW/Chi also) was that the system was unbreakable without capturing at least some indicators and probably the machine itself. A TYPEX machine was captured in 1940 at either BREST or DUNKIRK, but without drums, and was therefore useless. TRANOW mentions that throughout researches on TYPEX, messages were always too short to enable even hope of a break and the number of indicators was extremely large, thus reducing to almost nothing the chance of finding two messages on the same setting. He mentioned two personalities at OKW/Chi who were regarded as experts on machine systems, and also worked on TYPEX, a Dr. HUETTENHAIN and a Dr. STEINBACH, who, at the time of the collapse, were certainly in the BRITISH Zone.

3. U.S. System with Indicator DUPYH

DUPYH was readable shortly after the outbreak of war in the PACIFIC for roughly 12 months, owing to the fact that the Japanese captured all necessary documents and wirelessed all particulars to GERMANY. The Eliminator Tables covered roughly a year, and when they had run out, reading ceased. The content of the messages dealing with events in the PACIFIC had little more than an academic interest, and therefore, no effort was later made to break the system cryptographically. In any case, SCHULZE's opinion is that it is unbreakable. He points out how extremely long it takes both to encipher and decipher. After the first information, they never received anything further from the Japanese.

4. U.S. NAVY Call-Signs.

No success was achieved on the identification or breaking of US NAVY Call-Signs, and SCHULZE does not think ever could have been, although it is true that research was begun very late with very few people.

Please turn over

A changing call-sign could be followed from day to day, of course, the internal addresses, such as: TUBA NITE, etc. being of use.

They were certainly considered to be enciphered on a frequently changing hatted alphabet and figure sequence.

5. Captured Machines.

The only captured machine in 4 SKL III was the HAGELIN, which had been found in DENMARK. SCHULZE states that he has already been interrogated regarding his work and complete success on this machine. As stated above, he did a certain amount of preliminary work on TYPEX and Verfahren ULM, without success.

6. KORVETTEN KAPITAEN SINGER.

SINGER was a mathematician and expert on the ENIGMA machine. In the summer of 1944, there was apparently a certain disquiet as to the possibility that the British were having some success, although nothing definite was known. SINGER's department was devoted into research on the breakability of the machine, using similar methods to SCHULZE's on HAGELIN. The work was considered sufficiently important to rob SCHULZE of some 20 men from his department, much to his annoyance. SCHULZE does not know what conclusions SINGER reached, but in his opinion, if sufficient messages on the same setting were intercepted, it was probably breakable.

7. Liaison between different departments.

SCHULZE had very little information on this, and TRANOW had very little information either. It was apparently a matter of regret that departmental jealousies prevented any fruitful co-operation. OKW/Chi was generally considered the best department (certainly the most richly provided in personnel), 4 SKL III came next, followed by OKH and LUFTWAFFE respectively.

8. Other work carried out by SCHULZE.

SCHULZE also carried out researches on SWEDISH machine and hand systems. He had no success with any SWEDISH machines, their peculiarity being that cipher letter counts showed the same results as normal clear SWEDISH letter counts. He also noticed this occasionally in some of the lesser known and lesser used U.S. machine ciphers.

9. Deviation Percentage (PROZENTUALE STREUUNG)

Deviation Percenta was SCHULZE's method of initial research into new machine ciphers. At least 30,000 letters were first indexed. 30,000 was the minimum number of letters which produced consistent results. A percentage of the total for each individual letter was then worked out, and the lowest letter percentage was then subtracted from the highest letter percentage. The resultant percentage was the Deviation Percentage of the particular machine. A Deviation Percentage of over 2% indicated an insecure machine. The D.P. of HAGELIN, for instance, was from 1.2% to 1.6%, whereas that of ENIGMA was from 0.8% to 1.0%. Individual letter percentage graphs were kept of different machines, and served as useful comparisons.

Please turn over

TICOM

TOP SECRET

10. The Z-Strip (Z-Leiste)

The Z-Strip method is merely another refinement for distinguishing various machines one from another. After indexing 30,000 letters (see 9 above) the letters are placed in order, the highest appearance first. Each letter is then enciphered against the Z-Strip of a TRITTHEIM Table (see Appendix 1). The Z-Strip was chosen because clear Z was by far the most numerous letter in clear HAGELIN messages. Thus if the letter percentage order on a particular cipher was QWSXBGT etc., etc., comparison with the Z-Strip would give :

Q = Z = 17
W = Z = 23
S = Z = 19 etc.

It was a characteristic of HAGELIN that the smaller differences, such as 2, 3, 4, 5 came against letters R to V, etc. Deviation Percentage and Z-Strip investigations were the basis of distinction and comparison between all codes, machine and non-machine. SCHULZE mentions, in this connection, how the new Verfahren ULM was shown by this system to be distinct from TYPEX, and comments that ULM had various features in common with a SWEDISH machine on which he had once worked.

11. The A-Strip (A-Leiste)

The A-Strip was a method of breaking into HAGELIN when two different messages were enciphered on the same setting. Although the method was evolved by SCHULZE himself, he states that this seldom happened on NAVAL traffic. The ARMY, however, intercepted many such messages, and used his system with success.

Method of Working. In Fig. 1 of Appendix 2 are two messages, one beginning "REPORT POSITION", and one beginning "HMS BARHAM". Both messages are assumed to be enciphered on the same setting, and the "clear-cipher" differences are shown in red above. Cipher 1 and Cipher 2 indicate the enciphered messages. Using two sliding reciprocal alphabets, the cryptographer now prepares 26 vertical versions of message 2 on the assumption in each case that each letter in message 1 is clear A, clear B, etc. For example, if in message 1, cipher J equals clear A,* then N equals S, if W equals A, then Z equals X, etc., thus building up strip 1 in Fig. 2, under letter A, as KSXNRCIO, etc. The succeeding strips are built up on similar alphabetical assumptions. Fig. 2 is now cut up into 26 strips.

The cryptographer, using his knowledge of standard message beginnings, such as "YOUR, MY, REFERENCE, REPORT, REQUEST, HMS" etc. arranges the strips "staircase-wise" (treppenartig), the top letter of each strip representing the letters of a clear message. He then looks in the body of the strips horizontally for the elements of a clear word, which would represent the second message. In the example given in Fig. 3, HMS produces REP in the body of the strips. This is obviously REPORT, and by piecing the missing ORT from other strips thereto, he produces BAR at the top. Knowing of a ship BARHAM, he is then able to add strips HAM, thus giving him the letters POS next to REPORT in the body of the strips. Continuing in this manner, the two messages gradually emerge.

12. Machine Systems OTTO, SOPHIE, KARL, PAUL, RICHARD and hand systems SASSNITZ, HGA, SEDER, ZBB, FFF, FFFF were all SWEDISH systems.

* Please insert: then in message 2, cipher Z equals clear K, if F equals A,

Please turn over

13. Conclusion.

SCHULZE's main successes were on the BRITISH NAVAL Subtractor Code, using a fixed book of subtractor tables for a considerable time (SCHULZE refers to this book as a WURM), and on the HAGELIN machine. He states he has already been exhaustively interrogated on these systems.

Quite obviously, no really intensive work was carried out by 4 SKL III on any other machine systems, although from time to time, ineffectual attempts were made on TYPEX, UIM, etc. and on SWEDISH machines. HUETTENHAIN and STEINBACH know more about machine ciphers other than HAGELIN than either SCHULZE or TRANOW. There was, incidentally, a HOLLERITH component at 4 SKL III. The HOLLERITH machine is apparently made under license in GERMANY.

SCHULZE is an intelligent man of 44 years of age, who appears to have quite an original mind, although no highly trained formal mathematician. Like so many other German cryptographers, he would undoubtedly be delighted to continue in some form or another his cryptographic activities.

On the question of liaison with other departments, of which field both SCHULZE and TRANOW seemed able to say so little, no doubt KUPFER, who was head of the whole department, would know more. He was away at the time of my visit to HAMBURG, and I was unable to see him. According to SCHULZE, however, his activities were purely organisational and he is no technician.

22nd June, 1946.

Appendices 1 and 2 attached.

APPENDIX 1 - TRITHEIM TABLE

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	A
B	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	B
C	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	C
D	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	D
E	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	E
F	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	F
G	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	G
H	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	H
I	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	I
J	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	J
K	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	K
L	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	L
M	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	13	M
N	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	14	N
O	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	15	O
P	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	16	P
Q	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	17	Q
R	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	18	R
S	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	19	S
T	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	20	T
U	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	21	U
V	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	22	V
W	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	23	W
X	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	24	X
Y	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	25	Y
Z	25	24	23	22	21	10	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Z
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

TOP SECRET

APPENDIX 2 - DIE A-LEISTE.

FIG. 1

CIPHER DIFFERENCES	18	1	7	11	12	5	7	9	6	10	etc						
CLEAR 1.	R	E	P	O	R	T	P	[illegible]	S	T	[illegible]	T	O	N	etc		
CLEAR 2.	H	M	S	B	A	R	H	A	M	etc							
CIPHER 1.	J	F	W	Z	D	Y	W	X	A	S	etc						
CIPHER 2.	Z	N	Z	M	M	W	O	J	U	etc							

FIG. 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N

FIG. 3

					18
				I	R
			2	A	B
		19	B	K	J
	13	S	L	S	O
8	M	C	T	X	E
H	W	K	Y	N	I
R	E	P	O	R	T
Z	J	F	S	C	Z
E	Z	J	D	I	F
U	D	U	J	O	
Y	O	A	P		
J	U	G			
P	A				
V					